

Security schedule

Version	1.0
Effective date	27 October 2026
Owner	Robin Ashford
Applies to	The Final Frame platform, as offered to customers. Annex C to the data processing agreement
Review	27 October 2027
MPA CSBP	OR-3.4, PS-3.3

Approved by Robin Ashford, Founder, 27 October 2026

This schedule describes the technical and organisational measures in place on the date above. Final Frame is preparing for a Trusted Partner Network (TPN) assessment against the MPA Content Security Best Practices v5.3.1. The assessment has not taken place. Final Frame holds no SOC 2 report and no ISO 27001 certificate.

Governance

- Robin Ashford, founder, is the security owner. He approves policies, accepts or rejects risks, leads incident response and reviews access.
- A written policy set covers information security, acceptable use, access control, change management, secure development, logging and monitoring, incident response, business continuity, availability, data classification, retention and disposal, vendor management, AI use, workstations and penetration testing. The founder approved the set on 27 October 2026. Each policy is reviewed at least every 12 months.
- Everyone with access completes a security awareness module before access and every 12 months, and each completion is recorded.
- Final Frame claims no certification it does not hold.

Access control

- Access to customer data comes only from a membership: a user, an Org, a scope (the Org, a Group or a Project) and a role. Access inherits down the Group tree.
- Accounts are created by invitation from an Org administrator. There is no self-service sign-up into an Org.
- Roles are bundles of permissions: Admin, Editor and Viewer. The server checks the permission on every request. A route with no policy is denied.
- Removing a membership ends that person's access on their next request. A password reset revokes every session for the account.
- Final Frame staff access to customer data is limited to the platform administrator (Robin Ashford). "View as" support access is used only to answer that Org's support request or to investigate an incident. Each use writes impersonation.started and impersonation.ended to the Org's own audit trail, naming the person behind it. Impersonation sessions last at most 30 minutes.
- No administrative tool reads another Org's storage.

- Service identities authenticate through Google Cloud's metadata server. No service account key files exist.
- **Screening Room guests.** An Org may invite people at other companies into its Screening Room. A guest is never a member and holds no account. A guest sees only what that Org's grants show them, in that Org's room, and never a title the Org marks internal. Revoking a guest ends their sessions and anything they are playing at once; their access also ends at its expiry.

Authentication and sessions

- Users sign in through WorkOS, with email and password and an authenticator-app code or the customer's own single sign-on (SAML or OIDC), or with a passkey that requires the device's own unlock. Multi-factor authentication is set to Required in WorkOS. Passkeys are the recommended method. Social sign-in (Google, Microsoft, Apple) is available, where the provider's own second factor applies.
- Sign-in routes are rate limited.
- Session tokens are 256-bit random values. Only a SHA-256 hash is stored.
- Sessions end after 15 minutes idle and 12 hours in all, enforced by the server. Background polling does not keep a session alive. The web app warns 60 seconds before an idle sign-out.
- The session cookie is __Host-session: HttpOnly, Secure, Path=/, no Domain, SameSite=Lax.
- Policy requires a second factor on every human account with access to production or customer data, at Final Frame and at its vendors, wherever the vendor offers one.
- Five wrong codes lock a guest for 15 minutes, and ten until the Org unlocks them. A guest session lasts 8 hours by default (24 at most) and ends after 60 minutes idle by default. Only a hash of each link and session token is stored.

Tenant isolation

- Each customer is an Org, and the Org is the isolation boundary.
- Every Org-scoped database table carries the Org id. PostgreSQL row-level security is enabled and forced on every such table. With no Org context, a query returns no rows.
- The application connects as a role that does not own the schema and cannot bypass row-level security. Schema changes run under a separate role.
- The Org a request names is checked against the user's membership before it is used.
- An automated isolation test suite runs on every code change and tests reads and writes across Orgs, on every table that carries the Org id. A second test checks that every API route refuses a signed-out request and a member of another Org.
- Each Org has its own Cloud Storage bucket, encrypted with its own Cloud KMS key. Buckets use uniform bucket-level access, and public access is prevented.

Encryption

Data	In transit	At rest
Media and files in Org buckets	TLS 1.2 or higher. Transfers use signed URLs for one object, 15 minutes by default, 60 minutes at most	Per-Org customer-managed key (Cloud KMS, AES-256), rotated every 90 days
Temporary reading copies for model calls	TLS	Final Frame-managed Cloud KMS key, rotated every 90 days. Deleted within one day

Data	In transit	At rest
Database (Cloud SQL PostgreSQL)	Encrypted connections enforced, through the Cloud SQL connector only	Google-managed keys, AES-256
Secrets	TLS	Google Secret Manager
Customer cloud storage credentials	TLS, to the customer's provider only	AES-256-GCM, a fresh data key per credential, wrapped by a Cloud KMS key rotated every 90 days

- The public load balancer accepts TLS 1.2 and above only (Google's MODERN profile).
- Web responses carry HSTS (one year, with subdomains), X-Frame-Options: DENY, nosniff and a strict referrer policy.
- Media bytes never pass through the API. Signed URLs are never written to logs.

Logging and audit trail

- **Audit trail.** An append-only record per Org of uploads, receipts, removals, deliveries, download links issued from the app and the API, status changes, memberships, roles, invitations, settings and impersonation. The application cannot change or delete an entry. It is kept for the life of the Org and offered as an export before the Org is closed.
- **Screening Room viewing records.** Every guest sign-in, and every title view and play in the Screening Room by members and guests, is recorded in an append-only log of its own, with the IP address and browser. Reads and exports of its analytics are in the audit trail.
- **Request and security logs.** One structured line per request, with request id, Org, actor, impersonator, route, duration and outcome. Application, Cloud KMS, Cloud Storage, IAM and Secret Manager logs are kept for 365 days in a log bucket whose retention is locked.
- **Cloud audit logs.** Changes to Google Cloud configuration and IAM are kept for 400 days, locked. Access to Cloud KMS keys and secrets, and writes to Cloud Storage, are logged.
- **Never logged.** Passwords, secrets, session cookies, tokens, API keys, signed URLs, full request bodies and media contents. Both application loggers remove credentials and signed URL signatures before a line is written, and every code change is checked for a log call that passes a request body, headers, cookies or a signed URL.
- **Monitoring.** Uptime checks, and alerts on server errors, database connections, database load, database recovery, rate-limited traffic, job volume, repeated failed sign-ins, support access ("View as"), platform administrator actions and the creation of service account or HMAC keys, notify the security owner by email.
- All timestamps are UTC from Google's time source.

Vulnerability management

- Every code change runs a dependency vulnerability audit of shipped packages. A high or critical advisory fails the build.
- Dependency updates are proposed weekly by Dependabot.
- Static analysis (CodeQL) and a secret scan of the whole repository history run daily and on every pull request. A finding fails the run.
- Every container image pushed to the registry is scanned for vulnerabilities by Google Artifact Registry.
- Each build produces a CycloneDX software bill of materials.

- Critical vulnerabilities are patched within 14 days and high within 30, or the risk is accepted in writing with a reason.
- Files filed to a project, other than picture and sound and files over 512 MB, and every project inbox attachment are scanned with ClamAV. An infected file is blocked and every link to it refused.
- An independent penetration test by a CREST-accredited firm covers the web application, API, MCP server and Mac app endpoints before production carries a customer's production workload, then yearly and after any major change. An internal review against the same scope comes before each test.

Change management

- Every change to the platform is a commit in a private Git repository.
- Continuous integration runs on every change: type checks, lint, unit tests, the tenant isolation suite, API integration tests, the dependency audit and the build.
- Deploys build from the main branch only, refuse uncommitted or unpushed code and reused version tags, and check that the new version is serving.
- One deploy runs at a time, under a lock, and each release is recorded in a release manifest. A new API version is smoke-tested with no traffic before it takes any.
- Each part of the platform (API, jobs, app, website) rolls back on its own in one command, within minutes.
- Deploys are frozen during client demonstrations and penetration test windows.
- Database migrations are forward only and run under a separate privileged role.
- Changes to Google Cloud configuration are recorded in the cloud audit logs.

Incident response and notification

- A written incident response plan defines incidents, four severity levels, containment steps, evidence preservation and review.
- Severity 1 (customer content or credentials exposed, or access across Orgs): affected customers are notified within 24 hours of confirmation.
- Severity 2 (likely exposure, or the platform unavailable): affected customers are notified within 48 hours of confirmation.
- Notice goes by email to the customer's named security contact, followed by a written report after review. The report gives root cause, timeline and the changes made.
- Final Frame acts as processor. The customer, as controller, decides on notifying the Information Commissioner's Office within 72 hours, and Final Frame gives it the information to do so.
- Every incident is reviewed within 10 working days.

Business continuity and disaster recovery

- The database runs in europe-west2, highly available across two zones with automatic failover. Point-in-time recovery is on, with 7 days of transaction logs. Automated daily backups are taken and 30 are kept. Deletion protection is on.
- A restore into a separate instance was rehearsed on 7 October 2026 and took 8 minutes 40 seconds. Restores are rehearsed every quarter.
- Org buckets keep deleted or overwritten objects for 30 days (soft delete).
- Customers keep their own originals.

Scenario	Recovery point	Recovery time
Faulty release	No data loss	15 minutes
Records deleted or corrupted	Under 5 minutes	4 hours
Object deleted or overwritten	No data loss, within 7 days	4 hours
Database zone failure	No data loss	15 minutes
Database instance failure	Under 5 minutes	4 hours
Loss of the europe-west2 region	Database: 24 hours.	48 hours

- Final Frame is run by one person. A sealed recovery pack, held by a named trusted person, is the route to continued access if he is unavailable.
- Affected customers are emailed when an outage passes one hour, and again when it ends.

Data location, retention and disposal

- Customer content and database records are stored in Google Cloud europe-west2 (London).
- Processing that can take place elsewhere is listed in Annex B of the data processing agreement.
- Customer content is kept until the customer deletes it or the Org is closed. A deleted file is recoverable for 30 days, then deleted by Google.
- Expired sessions, password resets and invitations are purged 90 days after they end.
- Screening Room guest records and viewing records are kept until the Org is closed.
- **Ending an Org.** Final Frame offers an export of the customer's content and audit trail, then archives the Org. Thirty days after archiving, it closes the Org permanently: it empties and deletes the Org's buckets, deletes its storage identities and keys, schedules every version of its encryption key for destruction (destroyed 30 days later), and deletes its database records. Each step is recorded. A certificate of destruction is issued with a SHA-256 digest of the closure record.
- Database backups expire within the backup retention period.
- A legal hold suspends deletion for an Org in writing.

AI and model use

- Final Frame does not train or fine-tune any model on customer content, and uses only providers whose terms say they do not train on its inputs or outputs.
- Every model call is recorded with Org, project, user, kind, model, tokens, cost and duration. Prompts and answers are not stored in that record.
- A model's output is a proposal for a person to accept, change or reject. A model never passes a QC gate, sends a delivery, changes a permission or deletes anything.
- The in-app assistant acts with the permissions of the person using it. Its changes are recorded and can be undone.
- Models receive the least content that does the job: low-resolution reading copies and frames, never masters.
- Each project chooses which content-reading features it uses. The model providers and what each receives are listed in Annex B.

Subprocessors and vendors

- Every outside service is listed in a vendor register with a tier set by what it receives.
- A vendor that receives customer content needs a security attestation, data processing terms, a commitment not to train on Final Frame's data, a known region and retention, and breach notice terms before use. Vendors that receive personal data or credentials need data processing terms and a second factor on Final Frame's account.
- Vendor evidence is reviewed every 12 months.
- Customers receive 30 days' notice of a new subprocessor and may object (data processing agreement, clause 8).
- Google Cloud provides the physical security of the data centres, hardware and network under its own certified controls.

Personnel

- Final Frame has one person, its founder. There are no employees or contractors.
- Anyone given access later is screened (identity, right to work, references) as far as UK law allows, signs a confidentiality agreement and completes security training before access and every year after. Access is removed the same day they leave.
- AI coding assistants used to build the platform never receive customer content or production secrets, and their changes go through the same Git history and continuous integration as any other change.

Workstations

- Final Frame is built and run from two company Macs, with a phone used only as an authenticator.
- Policy requires on every Mac: FileVault full-disk encryption, screen lock after 5 minutes, automatic updates, the firewall on, Gatekeeper on, Find My on for remote wipe, and sharing services off.
- Customer content is not stored on a workstation except for a task that needs it, and is deleted when the task ends. It is never copied to removable media, personal cloud storage or a phone.
- A password manager with its own second factor holds every credential. Production secrets are not stored on disk.
- A lost or stolen device is handled as an incident: lock and wipe, revoke its sessions and rotate any secret it could read.

Final Frame Ltd · Registered in England and Wales · Company number 17413345 · www.final-frame.com/trust